IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

HOKKY TJAHJONO and MILES BLACK, individually and on behalf of all others similarly situated, Plaintiffs, v. WESTINGHOUSE AIR BRAKE TECHNOLOGIES CORPORATION, d/b/a WABTEC CORPORATION, Defendant.	Case No. 2:23-cv-00531-WSS **JURY TRIAL DEMANDED**

FIRST AMENDED CLASS ACTION COMPLAINT

Plaintiffs Hokky Tjahjono and Miles Black (collectively, "Plaintiffs") bring this Class Action Complaint on behalf of themselves, and all others similarly situated, against Defendant Westinghouse Air Brake Technologies Corporation, d/b/a Wabtec Corporation ("Wabtec" or "Defendant"), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to them, which are based on personal knowledge:

NATURE OF THE CASE

1. Plaintiffs bring this class action against Wabtec for its failure to properly secure and safeguard protected personally identifiable information, including without limitation, individuals' full names, dates of birth; non-US national ID numbers; non-US social insurance numbers or fiscal codes; passport numbers; IP addresses, Employer Identification Numbers; USCIS or Alien Registration Numbers; medical records and health insurance information; photographs; gender; and gender identity; salary; Social Security Numbers; financial account

information; payment card information; account usernames and passwords; biometric information; race and ethnicity; criminal convictions and offenses; sexual orientation; religious beliefs; and union affiliation (collectively, "PII"), for failing to comply with industry standards to protect information systems that contain PII, and for failing to provide timely notice of the breach to Plaintiffs and Class Members. Plaintiffs seek, among other things, damages, and orders requiring Wabtec to adopt reasonably adequate security practices and safeguards to prevent incidents like the unauthorized access from occurring in the future and for Wabtec to provide identity theft protective services to Plaintiffs and Class Members for their lifetimes, as Plaintiffs and Class Members will be at an increased risk of identity theft due to the conduct of Wabtec described herein.

2. Wabtec prides itself on being a leading global manufacturer of "state-of-the-art locomotives and rail systems."[1] "The firm's 2021 financial results give a revenue figure of $7.8 billion, reporting a staggering 20% of the world's freight being moved by the 23,000 of Wabtec's locomotives in global operation."[2] With over 150 years of experience, Wabtec defines itself as a leader in "safety, efficiency, reliability, innovation, and productivity."[3]

3. On or about December 30, 2022, Wabtec announced that it had been the subject of a successful ransomware attack that impacted sensitive information contained on the affected computer systems (the "Data Breach").[4]

---

[1] Bill Toulas, *Rail Giant Wabtec Discloses Data Breach After Lockbit Ransomware Attack*, BleepingComputer (Jan. 3, 2023), https://www.bleepingcomputer.com/news/security/rail-giant-wabtec-discloses-data-breach-after-lockbit-ransomware-attack/.
[2] *Id.*
[3] *About Wabtec,* Wabtec, https://www.wabteccorp.com/about-wabtec (last visited June 26, 2023).
[4] *Data Security Incident Update – Personal Data Breach Public Communication*, Wabtec (Dec. 30, 2022), https://www.wabteccorp.com/data-security-incident-update-personal-data-breach-public-communication ("Data Breach Notice").

4. Based on public information available to date, the information impacted by the Data Breach includes a wide swath of personal information, including individuals' full names, dates of birth; non-US national ID numbers; non-US social insurance numbers or fiscal codes; passport numbers; IP addresses, Employer Identification Numbers; USCIS or Alien Registration Numbers; medical records and health insurance information; photographs; gender; and gender identity; salary; Social Security Numbers; financial account information; payment card information; account usernames and passwords; biometric information; race and ethnicity; criminal convictions and offenses; sexual orientation; religious beliefs; and union affiliation.[5]

5. As a direct and proximate result of Defendant's failure to implement and follow basic security procedures, Plaintiffs' and Class Members' PII is now in the hands of cybercriminals who have leaked Plaintiffs' and Class Members' PII onto the dark web.

6. Plaintiffs and Class Members are now at a significantly increased and certainly impending risk of fraud, identity theft, intrusion of their health privacy, and similar forms of criminal mischief, risk which may last for the rest of their lives. Consequently, Plaintiffs and Class Members must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes.

7. Plaintiffs, on behalf of themselves and all others similarly situated, allege claims for negligence, negligence *per se*, breach of implied contract, unjust enrichment, and declaratory judgment. Plaintiffs seek damages and injunctive relief, including the adoption of reasonably sufficient practices to safeguard PII in Defendant's custody in order to prevent incidents like the

[5] *Id.*

Data Breach from reoccurring in the future and for Defendant to provide identity theft protective services to Plaintiffs and Class Members for their lifetimes.

PARTIES

8. Plaintiff Tjahjono is an adult who at all relevant times is a resident and citizen of the State of Texas. Plaintiff Tjahjono was an employee of Wabtec and received a Data Breach Notice from Defendant informing him that his PII had been exposed during the Data Breach.

9. Since the announcement of the Data Breach, Plaintiff Tjahjono has been required to spend his valuable time monitoring his various accounts in an effort to detect and prevent any misuses of his PII—time which he would not have had to expend but for the Data Breach. Plaintiff Tjahjono took these mitigation steps at Wabtec's direction as Defendant's Data Breach Notice encouraged him to "remain vigilant against incidents of identity theft and fraud by reviewing your financial account statements and credit reports for any anomalies."

10. As a result of the Data Breach, Plaintiff Tjahjono will continue to be at heightened and certainly impending risk for fraud and identity theft, and their attendant damages for years to come.

11. Plaintiff Miles Black resides and is domiciled in the state of Florida. He was an employee of Wabtec for approximately twenty (20) years. Plaintiff Black provided sensitive personal information to the Defendant for the purpose of employment, and received notice from the Defendant that such information was compromised in the Data Breach. Plaintiff Black assumed his personal information had been destroyed following his employment period with the Defendant. Upon being informed of the Data Breach, Plaintiff Black became extremely concerned and feared that not only his personal information, but also his children's personal information would be

misused. His exposure to the Data Breach has also caused Plaintiff Black to review his credit reports and financial accounts on a weekly basis.

12. Since the announcement of the Data Breach, Plaintiff Black has been required to spend his valuable time monitoring his various accounts in an effort to detect and prevent any misuses of his PII—time which he would not have had to expend but for the Data Breach. Plaintiff Black took these mitigation steps at Wabtec's direction as Defendant's Data Breach Notice encouraged him to "remain vigilant against incidents of identity theft and fraud by reviewing your financial account statements and credit reports for any anomalies."

13. As a result of the Data Breach, Plaintiff Black will continue to be at heightened and certainly impending risk for fraud and identity theft, and their attendant damages for years to come.

14. Defendant Wabtec is a Delaware corporation with a principal place of business located at 30 Isabella Street, Pittsburgh, Pennsylvania 15212. Defendant Wabtec operates under the fictious name, Wabtec Corporation.

JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of $5,000,000.00, exclusive of interest and costs, there are 100 or more members of the proposed class, and at least one member of the proposed class is a citizen of a state different than Defendant.

16. This Court has personal jurisdiction over Defendant because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District, and Defendant resides in this District.

17. Pursuant to 28 U.S.C. § 1391, this Court is the proper venue for this action because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District and Defendant resides in this District.

FACTUAL BACKGROUND

18. Wabtec is the "world's foremost rail technology company," leading "the way in creating a more sustainable freight and passenger transportation network."[6]

19. Wabtec employs over 27,000 employees in over 50 countries around the world.[7]

20. During individuals' course of employment with Wabtec, Defendant receives, creates, and handles PII, which includes, *inter alia*, individuals' full names; dates of birth; non-US national ID numbers; non-US social insurance numbers or fiscal codes; passport numbers; IP addresses; Employer Identification Numbers; USCIS or Alien Registration Numbers; medical records and health insurance information; photographs; gender and gender identity; salary; Social Security Numbers; financial account information; payment card information; account usernames and passwords; biometric information; race and ethnicity; criminal convictions and offenses; sexual orientation; religious beliefs; and union affiliation.

21. In order to work for Wabtec, employees must entrust their PII to Defendant, and in return, they reasonably expect that Defendant will safeguard their highly sensitive PII.

22. Even though Wabtec "is committed to and takes very seriously its responsibility to safeguard all data entrusted to it,"[8] Wabtec nevertheless employed inadequate data security measures to protect and secure the PII employees entrusted to it, resulting in the Data Breach and compromise of Plaintiffs' and Class Members' PII.

---

[6] *About Wabtec*, Wabtec, https://www.wabteccorp.com/about-wabtec (last visited June 26, 2023).
[7] *Id.*
[8] *Data Breach* Notice, *supra* note 4.

A. The Value of Private Information and Effects of Unauthorized Disclosure.

23. Wabtec was well aware that the PII it collects is highly sensitive and of significant value to those who would use it for wrongful purposes.

24. Wabtec also knew that a breach of its computer systems, and exposure of the PII stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PII was compromised.

25. These risks are not theoretical; in recent years, numerous high-profile breaches have occurred at businesses such as Equifax, Facebook, Yahoo, Marriott, Anthem, and many others.

26. PII has considerable value and constitutes an enticing and well-known target to hackers. Hackers can easily sell stolen data as there has been a "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[9]

27. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identity theft, and medical and financial fraud.[10]

28. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S. In 2021, there were 4,145 publicly disclosed data breaches,

[9] Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/.

[10] *What To Know About Identity Theft*, Fed. Trade Comm'n (Apr. 2021), https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft.

exposing 22 billion records. The United States specifically saw a 10% increase in the total number of data breaches.[11]

29. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2017, 2.9 million people reported some form of identity fraud compared to 5.7 million people in 2021.[12]

30. The ramifications of Wabtec's failure to keep Plaintiffs' and Class Members' PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[13]

31. Even if stolen PII does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name,

[11] *Data Breach Report: 2021 Year End*, Risk Based Security (Feb. 4, 2022), https://www.riskbasedsecurity.com/2022/02/04/data-breach-report-2021-year-end/.
[12] *Insurance Information Institute, Facts + Statistics: Identity theft and cybercrime*, Insurance Information Institute, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20 (last visited June 26, 2023).
[13] U.S. Gov't Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: https://www.gao.gov/new.items/d07737.pdf (last visited June 26, 2023).

address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

32. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Defendant's employees especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

33. **Social Security Numbers**—Unlike credit or debit card numbers in a payment card data breach—which can quickly be frozen and reissued in the aftermath of a breach—unique social security numbers cannot be easily replaced. Even when such numbers are replaced, the process of doing so results in a major inconvenience to the subject person, requiring a wholesale review of the person's relationships with government agencies and any number of private companies in order to update the person's accounts with those entities.

34. The Social Security Administration even warns that the process of replacing a Social Security number is a difficult one that creates other types of problems, and that it will not be a panacea for the affected person:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with

> your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[14]

35. Social Security Numbers allow individuals to apply for credit cards, student loans, mortgages, and other lines of credit—among other services. Often social security numbers can be used to obtain medical goods or services, including prescriptions. They are also used to apply for a host of government benefits. Access to such a wide range of assets makes social security numbers a prime target for cybercriminals and a particularly attractive form of PII to steal and then sell.

36. **Medical Records**—As indicated by Jim Trainor, former second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where PHI records can go from $20 say up to—we've even seen $60 or $70."[15] A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market, whereas stolen payment card information sells for about $1.[16]

37. Indeed, medical records "are so valuable because they can be used to commit a multitude of crimes. Healthcare data can be used to impersonate patients to obtain expensive medical services, Medicare and Medicaid benefits, healthcare devices, and prescription

---

[14] *Identify Theft and Your Social Security Numbers*, Social Security Admin. (June 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf.

[15] *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data*, *New Ponemon Study Shows*, IDX (May 14, 2015), https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat.

[16] *Managing cyber risks in an interconnected world, Key findings from The Global State of Information Security® Survey 2015*, PriceWaterhouseCoopers, https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf (last visited June 26, 2023).

medications. Healthcare records also contain the necessary information to allow fraudulent tax returns to be filed to obtain rebates."[17]

38. "In contrast to credit card numbers and other financial information, healthcare data has an incredibly long lifespan and can often be misused for long periods undetected. Credit card companies monitor for fraud and rapidly block cards and accounts if suspicious activity is detected, but misuse of healthcare data is harder to identify and can be misused in many ways before any malicious activity is detected. During that time, criminals can run up huge debts – far more than is usually possible with stolen credit card information."[18]

39. According to Experian:

> Having your records stolen in a healthcare data breach can be a prescription for financial disaster. If scam artists break into healthcare networks and grab your medical information, they can impersonate you to get medical services, use your data open credit accounts, break into your bank accounts, obtain drugs illegally, and even blackmail you with sensitive personal details.
>
> ID theft victims often have to spend money to fix problems related to having their data stolen, which averages $600 according to the FTC. But security research firm Ponemon Institute found that healthcare identity theft victims spend nearly $13,500 dealing with their hassles, which can include the cost of paying off fraudulent medical bills.
>
> Victims of healthcare data breaches may also find themselves being denied care, coverage or reimbursement by their medical insurers, having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores. In the worst cases, they've been threatened with losing custody of their children, been charged with drug trafficking, found it hard to get hired for a job, or even been fired by their employers.[19]

---

[17] Steve Alder, Editorial: *Why Do Criminals Target Medical Records*, HIPAA Journal (Oct. 14, 2022), https://www.hipaajournal.com/why-do-criminals-target-medical-records/#:~:text=Healthcare%20records%20are%20so%20valuable,credit%20cards%20in %20victims'%20names.

[18] *Id.*

[19] Brian O'Connor, *Healthcare Data Breach: What to Know About them and What to Do After One*, EXPERIAN (June 14, 2018), https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/.

40. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[20]

41. **Health Insurance Information**—"stolen personal health insurance information can be used by criminals to obtain expensive medical services, devices and prescription medications, as well as to fraudulently acquire government benefits like Medicare or Medicaid."[21]

42. Even if stolen PII or PHI does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII and PHI about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

43. **Passport Numbers**—As explained by Aura, a leading identity theft protection service, "[p]assports are among the most widely accepted forms of identification, making them prime targets for scammers and fraudsters. If scammers steal your passport number, they can

[20] U.S. Gov't Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: https://www.gao.gov/new.items/d07737.pdf (last visited June 26, 2023).
[21] Kate O'Flaherty, W*hy cyber-Criminals Are Attacking Healthcare -- And How to Stop Them*, Forbes (Oct. 5, 2018), https://www.forbes.com/sites/kateoflahertyuk/2018/10/05/why-cyber-criminals-are-attacking-healthcare-and-how-to-stop-them/?sh=54e8ed1e7f69.

impersonate you, create rake travel documents, or even open bank accounts in your name."[22] Indeed, when combined with other PII, such as a name, address, or picture, a "passport number enables scammers to impersonate you, access your online accounts, or target you in sophisticated scams that lead to identity theft."[23]

44. Moreover, "[u]nlike credit card data or personal Social Security numbers, there are few mechanisms in place to alert consumers that their passport numbers have been stolen and possibly used for fraud" making it difficult to determine if criminals are suing a forged or fraudulent passport in an individual's name.[24]

45. **Financial Account Information**—Stolen financial account can have an equally devasting impact on consumers. Cybercriminals can deplete and wipe out a person's life savings or take out a loan or mortgage against someone's home with the click of a button. Indeed, stolen financial account information can be used to transfer money from a victim's bank account to another; to make purchases on online shopping sites; file fake tax returns; and create and use fraudulent checks.[25]

46. **Payment Card Information**—Cybercriminals can use stolen payment card information to create counterfeit payment cards and make unauthorized charges or withdrawals that can cause consumers to incur significant financial losses. Indeed, the counterfeit payment cards (or the compromised payment card information itself) can be used to purchase high-ticket

---

[22] Yaniv Masjedi, *What Can Scammers Do With Your Passport Number*?, Aura (Apr. 12, 2023), https://www.aura.com/learn/what-can-someone-do-with-your-passport-number#:~:text=If%20scammers%20steal%20your%20passport,could%20still%20be%20at%20risk.

[23] *Id.*

[24] Kate Fazzini, *Here's how criminals use stolen passport information*, CNBC (July 5, 2019), https://www.cnbc.com/2019/07/05/how-criminals-use-stolen-passport-information.html.

[25] Anthony Aguilar, *What Can Scammers Do With Your Bank Account Number*, Aura (Oct. 5, 2022), https://www.aura.com/learn/what-can-someone-do-with-your-bank-account-number.

goods or gift cards that can then be sold for cash all while charging the consumer's original card. Cybercriminals can also sell the stolen payment card information to other cybercriminals on the dark web. In turn, when a payment card is fraudulently used, it can damage the cardholder's credit score, making it difficult to obtain new credit in the future.

47. Based on the value of its employees' PII to cybercriminals, Wabtec knew or should have known, the importance of safeguarding the PII entrusted to it and of the foreseeable consequences if its data security systems were breached. Wabtec failed, however, to take adequate cyber security measures to prevent the Data Breach from occurring.

B. Manufacturing Companies are Particularly Vulnerable to Data Breaches.

48. Wabtec also knew or should have known that manufacturing companies, such as itself, have become prime targets for cybercriminals.

49. "As an industry, manufacturers are one of the least technology mature industries, regularly outpaced by companies in media, finance and healthcare. Among global manufacturers, only 24% have implemented a smart manufacturing initiative, and just another 22% are in the pilot stages. That leaves more than half of global manufacturers relying on systems and processes that haven't kept up with modern security measures."[26]

50. "This lagging security expertise, combined with a low tolerance for disruption, has set up manufacturers to be rising targets for cybercriminals."[27]

[26] Cathy Pitt, *Why Cybercriminal Target Manufacturers – And What to do About it, Security*, https://www.securitymagazine.com/articles/94030-why-cyber-criminals-target-manufacturers-and-what-to-do-about-it (last visited June 26, 2023).
[27] *Id.*

51. Indeed, IBM's annual X-Force Threat Intelligence Index reported that the manufacturing sector was the most targeted industry for cyberattacks in 2021, dethroning the financial services and insurance industry as the most attacked industry.[28]

52. Cybercriminals have further targeted manufacturing companies in part because of the critical role these companies play in the global supply chain and because successful attacks against manufacturing companies immediately create problems in the production and supply chain, making it more likely that cybercriminals can demand lucrative ransoms.[29]

53. Put differently, cybercriminals target the manufacturing industry because disrupting the supply chain "strikes at the heart of a manufacturer's ability to meet customer orders and grow revenue. Many manufacturers quietly pay the ransom because they have no other choice."[30]

C. Defendant Breached its Duty to Protect its Employees' PII.

54. On June 26, 2022, Wabtec detected unusual activity on its network leading to an investigation of the attack and whether the hackers had exfiltrated any data.[31]

[28] Chris Ehrilich, *Manufacturing is the 'Most Targeted' Industry for Cyber Attacks*, Datamation (Mar. 9, 2022), https://www.datamation.com/security/manufacturing-most-targeted-industry-cyber-attacks/.
[29] *Manufacturing Sector is the Most Popular Target of Cyber* Attacks, Cybersec Europe (Mar. 21, 2022), https://www.cyberseceurope.com/blog/artikel/manufacturing-sector-is-the-most-popular-target-of-cyber-attacks/.
[30] Louis Columbus, *The Manufacturing Industry's Security Epidemic Needs a Zero-Trust Cure*, Venture Beat (Nov. 15, 2022), https://venturebeat.com/security/the-manufacturing-industrys-security-epidemic-needs-a-zero-trust-cure/.
[31] *Data Breach Notice*, *supra* note 4.

55. The next day, news outlets reported that sources at one of Wabtec's manufacturing plants indicated that it was a ransomware attack impacting the rail giant. However, the company did not officially respond to the rumors.[32]

56. Wabtec subsequently discovered that on or about March 15, 2022, cybercriminals had introduced malware into certain Wabtec systems.[33]

57. On or about November 23, 2022, nearly five months after the Data Breach occurred, Wabtec concluded its investigation and determined that certain systems containing personal information were subject to unauthorized access.[34] Wabtec further determined that personal information contained in the impacted systems was exfiltrated by cybercriminals.[35]

58. The information impacted by the Data Breach includes a wide swath of personal information, including individuals' full names; dates of birth; non-US national ID numbers; non-US social insurance numbers or fiscal codes; passport numbers; IP addresses; Employer Identification Numbers; USCIS or Alien Registration Numbers; medical records and health insurance information; photographs; gender and gender identity; salary; Social Security Numbers; financial account information; payment card information; account usernames and passwords; biometric information; race and ethnicity; criminal convictions and offenses; sexual orientation; religious beliefs; and union affiliation.[36]

---

[32] Lisa Adams, *Possible Ransomware Attack Allegedly Impacted Wabtec*, Erie News Now (June 27, 2022), https://www.erienewsnow.com/story/46773012/possible-ransomware-attack-allegedly-impacting-wabtec.
[33] Toulas, *supra* note 1.
[34] *Id.*
[35] *Id.*
[36] *Data Breach Notice*, *supra* note 4.

59. While Wabtec has not indicated the cybercriminals responsible for the Data Breach, the ransomware group, LockBit, has claimed responsibility for the Data Breach.[37]

60. A few weeks after news outsets reported that Wabtec was subject to a possible ransomware attack, LockBit published samples of data stolen from Wabtec on its ransomware website.[38]

61. LockBit demanded that Wabtec pay up to $30 million dollars for the decryptor and to destroy the stolen documents.[39] After Wabtec presumably refused to pay the ransom, LockBit leaked all of the solen data on its ransomware website on or about August 20, 2022.[40]

62. The data posted on LockBit's disclosure site, identified as belonging to Wabtec, appears to be a combination of internal employee PII, partner/customer invoices, and non-employee PII data.[41]

63. Following the publishing of the exfiltrated data on LockBit's ransomware site, Wabtec waited approximately four additional months and began notifying affected Class Members, including Plaintiffs, of the Data Breach on or around December 30, 2022.[42] As such, Plaintiffs and Class Members were not informed for nearly six months after the Data Breach occurred that their PII entrusted to Wabtec was compromised.

---

[37] Toulas, *supra* note 1.
[38] *Id.*
[39] Prajeet Nair, *Wabtec Discloses Data Breach; LockBit Claims Responsibility*, Bank Info Security (Jan 4, 2023), https://www.bankinfosecurity.com/wabtec-discloses-data-breach-lockbit-claims-responsibility-a-20853.
[40] Toulas, *supra* note 1.
[41] Steve Zurier, *Wabtec Breach Linked to LockBit Ransomware Group*, SC Media (Jan 4, 2023), https://www.scmagazine.com/news/ransomware/wabtec-breach-linked-to-lockbit-ransomware-group.
[42] *Data Breach Notice*, *supra* note 4.

64. In its notice to Plaintiffs and the Class, Wabtec provided them with a mere two-years of credit monitoring services, even though their PII was leaked on the dark web by a ransomware group, subjecting them to a lifelong risk of identity theft.

65. On or around the same time, Wabtec reported the Data Breach to the Office of the Main Attorney General indicating that the Data Breach impacted, at a minimum, 7,415 individuals.[43]

66. The Data Breach is the direct and proximate result of Wabtec's failure to implement reasonable data security measures and follow its own policies in order to protect the PII in its custody.

67. Upon information and belief, Wabtec breached its duties through some combination of the following errors and omissions that allowed the data compromise to occur: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of employee information that resulted in the unauthorized access and compromise of PII; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the Data Breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own internal policies or procedures; and (h) failing to adequately train and supervise

[43] *Data Breach Notifications*, Office of the Maine Attorney General, *https*://apps.web.maine.gov/online/aeviewer/ME/40/0e0731d8-10b1-4365-8a06-169bfd34832e.shtml (last visited June 26, 2023).

employees and third party vendors with access or credentials to systems and databases containing sensitive PII.

D. FTC Guidelines Prohibit Wabtec from Engaging in Unfair or Deceptive Acts or Practices.

68. Wabtec is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

69. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[44]

70. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[45]

71. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity

[44] *Start with Security – A Guide for Business*, United States Federal Trade Comm'n (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.
[45] *Protecting Personal Information: A Guide for Business*, United States Federal Trade Comm'n, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

on the network; and verify that third-party service providers have implemented reasonable security measures.[46]

72. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

73. Wabtec failed to properly implement basic data security practices. Wabtec's failure to employ reasonable and appropriate measures to protect against unauthorized access to employee PII constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

74. Wabtec was at all times fully aware of its obligations to protect the PII of its employees because of its position as an employer, which gave it direct access to reams of employee PII. Defendant was also aware of the significant repercussions that would result from its failure to do so.

E. Plaintiffs and Class Members Suffered Damages.

75. The ramifications of Wabtec's failure to keep PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years. Plaintiffs and Class Members now face years of constant surveillance of their personal records, monitoring, and loss of rights.

76. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason, Plaintiffs and Class Members will need to maintain these heightened measures for years, and possibly their entire lives

[46] *Id.*

as a result of Defendant's conduct. Further, the value of Plaintiffs' and Class Members' PII has been diminished by its exposure in the Data Breach.

77. Plaintiffs and Class Members are at substantial increased risk of suffering identity theft and fraud or misuse of their PII as a result of the Data Breach. From a recent study, 28% of consumers affected by a data breach become victims of identity fraud—this is a significant increase from a 2012 study that found only 9.5% of those affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identity fraud is only about 3%.[47]

78. Besides the monetary damage sustained in the event of identity theft, Plaintiffs and Class Members may have to spend hours trying to resolve identity theft issues. For example, the FTC estimates that it takes consumers an average of 200 hours of work over approximately six months to recover from identity theft.[48]

79. Plaintiffs and Class Members are also at a continued risk because their information remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as Defendant fails to undertake the necessary and appropriate security and training measures to protect its users' PII.

80. Plaintiffs and Class Members have suffered emotional distress as a result of the Data Breach, the increased risk of identity theft and financial fraud, and the unauthorized exposure of their private information to strangers.

---

[47] Stu Sjouwerman, *28 Percent of Data Breaches Lead to Fraud*, KnowBe4, https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud (last visited June 26, 2023).

[48] Kathryn Parkman, *How to Report identity Theft*, ConsumerAffairs (Feb. 17, 2022), https://www.consumeraffairs.com/finance/how-to-report-identity-theft.html.

81. As a result of Defendant's failure to prevent the Data Breach, Plaintiffs and Class Members have sustained and will continue to sustain economic loss and other harm. They have experienced and/or face an increased risk of experiencing the following forms of injuries:

a. Money and time expended to prevent, detect, contest, and repair identity theft, fraud, and other unauthorized uses of PII;

b. Money and time lost as a result of fraudulent access to and use of their financial accounts;

c. Loss of use and access to their financial accounts and/or credit;

d. Money and time expended to order credit reports and place temporary freezes on credit, and to investigate option for credit monitoring and identity theft protection services;

e. Money and time expended to avail themselves of assets and/or credit frozen or flagged due to misuse;

f. Impairment of their credit scores, ability to borrow, and/or ability to obtain credit;

g. Money and time expended to ameliorate the consequences of the filing of fraudulent income tax returns, including by completing paperwork associated with the reporting of fraudulent returns and the manual filing of replacement returns;

h. Lost opportunity costs and loss of productivity from efforts to mitigate and address the adverse effects of the Data Breach, including efforts to research how to prevent, detect, contest, and recover from misuse of PII;

i. Anticipated future costs from the purchase of credit monitoring and identity theft protection services; and

j. Loss of the opportunity to control how their PII is used.

CLASS ALLEGATIONS

82. Plaintiffs bring this class action on behalf of themselves and all other individuals who are similarly situated pursuant to Rule 23 of the Federal Rules of Civil Procedure.

83. Plaintiffs seek to represent a class of persons to be defined as follows:

> All individuals in the United States whose PII and/or PHI was compromised in the Wabtec Data Breach which was announced on or about December 30, 2022 (the "Class").

84. Excluded from the Class are Defendant, its subsidiaries and affiliates, officers and directors, any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

85. This proposed class definition is based on the information available to Plaintiffs at this time. Plaintiffs may modify the class definition in an amended pleading or when they move for class certification, as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

86. **Numerosity:** Plaintiffs are informed and believe, and thereon allege, that there are at minimum, thousands of members of the Class described above. The exact size of the Class and the identities of the individual members are identifiable through Defendant's records, including but not limited to the files implicated in the Data Breach, but based on public information, the Class includes thousands of individuals.

87. **Commonality:** This action involved questions of law and fact common to the Class. Such common questions include but are not limited to:

a. Whether Defendant had a duty to protect the PII of Plaintiffs and Class Members;

b. Whether Defendant was negligent in collecting and storing Plaintiffs' and Class Members' PII, and breached its duties thereby;

c. Whether Plaintiffs and Class Members are entitled to damages as a result of Defendant's wrongful conduct; and

d. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct.

88. **Typicality:** Plaintiffs' claims are typical of the claims of the members of the Class. The claims of the Plaintiffs and members of the Class are based on the same legal theories and arise from the same unlawful and willful conduct. Plaintiffs and members of the Class were all employees of Defendant, each having their PII exposed and/or accessed by an unauthorized third party.

89. **Adequacy of Representation:** Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the members of the Class. Plaintiffs will fairly, adequately, and vigorously represent and protect the interests of the members of the Class and have no interests antagonistic to the members of the Class. In addition, Plaintiffs have retained counsel who are competent and experienced in the prosecution of class action litigation. The claims of Plaintiffs and the Class Members are substantially identical as explained above.

90. **Superiority:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this

controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense, and promote uniform decision-making.

91. **Predominance:** Common questions of law and fact predominate over any questions affecting only individual Class Members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendant's liability and the fact of damages is common to Plaintiffs and each member of the Class. If Defendant breached its duty to Plaintiffs and Class Members, then Plaintiffs and each Class member suffered damages by that conduct.

92. **Injunctive Relief:** Defendant has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. Civ. P. 23 (b)(2).

93. **Ascertainability:** Members of the Class are ascertainable. Class membership is defined using objective criteria, and Class Members may be readily identified through Defendant's books and records.

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiffs and the Class)

94. Plaintiffs restate and reallege all preceding factual allegations above as if fully set forth herein.

95. Defendant owed a duty under common law to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. More specifically, this duty including, among other things: (a) designing, maintaining, and testing its security systems to ensure that Plaintiffs' and Class Members' PII in Defendant's possession was adequately secured and protected; (b) implementing processes that would detect a breach of its security system in a timely manner; (c) timely acting upon warnings and alerts, including those generated by its own security systems, regarding intrusions to its networks; and (d) maintaining data security measures consistent with industry standards.

96. Wabtec's duty to use reasonable care arose from several sources, including but not limited to those described below.

97. Defendant had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Defendant. By collecting and storing valuable PII that is routinely targeted by cyber-criminals for unauthorized access, Defendant was obligated to act with reasonable care to protect against these foreseeable threats.

98. Wabtec's duty also arose from Defendant's position as an employer of Plaintiffs and Class Members. During the course of employment, Plaintiffs and Class Members were required to provide Defendant with their PII and Defendant thereby assumed a duty to reasonably protect its employees' PII. Indeed, Wabtec was in a unique and superior position to protect from the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

99. Defendant breached the duties owed to Plaintiffs and Class Members and thus was negligent. Defendant breached these duties by, among other things, failing to: (a) exercise

reasonable care and implement adequate security systems, protocols and practices sufficient to protect the PII of Plaintiffs and Class Members; (b) detect the Data Breach while it was ongoing; (c) maintain security systems consistent with industry standards; and (d) disclose that Plaintiffs' and Class Members' PII in Defendant's possession had been, or was reasonably believed to have been, stolen or compromised.

100. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, their PII would not have been compromised.

101. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered injuries, including:

a. Theft of their PII;

b. Costs associated with requested credit freezes;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of the PII;

d. Costs associated with purchasing credit monitoring and identity theft protection services;

e. Lowered credit scores resulting from credit inquiries following fraudulent activities;

f. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

g. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of cyber-criminals;

h. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others; and

i. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' PII.

102. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION
NEGLIGENCE PER SE
(On Behalf of Plaintiffs and the Class)

103. Plaintiffs restate and reallege all preceding factual allegations above as if fully set forth herein.

104. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by institutions such as Defendant or failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

105. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with the industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a data breach within the manufacturing sector.

106. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

107. Plaintiffs and Class Members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) was intended to protect.

108. Moreover, the harm that has occurred is the type of harm that the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and Class Members.

109. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Class)

110. Plaintiffs restate and reallege all preceding allegations above as if fully set forth herein.

111. Wabtec required Plaintiffs and Class Members to provide their PII as a condition of their employment.

112. As a condition of their employment with Wabtec, Plaintiffs and Class Members provided their PII to Defendant. In doing so, Plaintiffs and Class members entered into implied

contracts with Wabtec by which Defendant agreed to safeguard and protect such PII, keep such PII secure and confidential, and to timely and accurately notify Plaintiffs and Class Members if their PII had been breached, compromised, or stolen.

113. When entering into these implied contracts, Plaintiffs and Class Members reasonably believed and expected that Wabtec's data security practices complied with its statutory and common law duties to adequately protect Plaintiffs' and Class Members' PII and to timely notify them of a data breach.

114. Indeed, implicit in these exchanges was a promise by Defendant to ensure the PII of Plaintiffs and Class Members in its possession would be used to provide the agreed-upon compensation and other employment benefits from Defendant and that Wabtec would take adequate measures to protect Plaintiffs' and Class Members' PII and timely notify them in the event of a data breach.

115. It is clear by these exchanges that the parties intended to enter into an implied agreements supported by mutual assent. Plaintiffs and Class Members would not have disclosed their PII to Defendant but for the prospect of Defendant's promise of compensation and other employment benefits. Conversely, Wabtec presumably would not have taken Plaintiffs' and Class Members' PII if it did not intend to provide Plaintiffs and Class members compensation and other employment benefits.

116. Plaintiffs and Class Members would not have provided their PII to Wabtec had they known that Defendant would not safeguard their PII as promised, or provide timely notice of a data breach.

117. Plaintiffs and Class Members fully performed their obligations under their implied contracts with Wabtec.

118. Wabtec breached its implied contracts with Plaintiffs and Class Members by failing to safeguard Plaintiffs' and Class Members' PII and by failing to provide them with time and accurate notice of the Data Breach.

119. The losses and damages Plaintiffs and Class Members sustained, include, but are not limited to:

a. Theft of their PII;

b. Costs associated with requested credit freezes;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of the PII;

d. Costs associated with purchasing credit monitoring and identity theft protection services;

e. Lowered credit scores resulting from credit inquiries following fraudulent activities;

f. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

g. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of cyber-criminals;

h. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others; and

i. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' PII.

120. As a direct and proximate result of Wabtec's breach of contract, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

FOURTH CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Class)

121. Plaintiffs restate and reallege all preceding allegations above as if fully set forth herein.

122. Plaintiffs bring this claim in the alternative to their breach of implied contract claim.

123. By engaging in the conduct described in this Complaint, Wabtec has knowingly obtained and derived benefits from Plaintiffs and Class Members at Plaintiffs' and Class Members' expense, namely their labor and the profits gained therefrom, and actual monies and benefits under circumstances such that it would be inequitable and unjust for Defendant to retain.

124. By engaging in the acts and failures to act described in this Complaint, Wabtec has been knowingly enriched by the savings in costs that should have been reasonably expensed to protect the PII of Plaintiffs and the Class. Defendant knew or should that known that theft of

employee PII could happened, yet it failed to take reasonable steps to pay for the level of security required to have prevented the theft of its employees' PII.

125. By engaging in the conduct described in this Complaint Wabtec has knowingly obtained benefits from Plaintiffs and the Class under circumstances such that it would be inequitable and unjust for Defendant to retain them.

126. Wabtec's failure to direct profits derived from Plaintiffs' and Class members' labor toward safeguarding Plaintiffs' and Class Members' PII constitutes the inequitable retention of a benefit without payment for its value.

127. Defendant will be unjustly enriched if it is permitted to retain the benefits derived from the theft of Plaintiffs' and Class members' PII.

128. Plaintiffs and Class Members have no adequate remedy at law. As a direct and proximate result of Wabtec's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

129. Wabtec should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them.

FIFTH CAUSE OF ACTION
DECLARATORY JUDGMENT
(On Behalf of Plaintiffs and the Class)

130. Plaintiffs restate and reallege all preceding allegations above as if fully set forth herein.

131. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

132. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and Class Members' PII and whether Wabtec is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their PII. Plaintiffs allege that Wabtec's data security measures remain inadequate, Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their PII and remains at imminent risk that further compromises of their PII will occur in the future.

133. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Wabtec owes a legal duty to secure employees' PII and to timely notify employees of a data breach under the common law, Section 5 of the FTC Act, and various state statutes; and

b. Wabtec continues to breach this legal duty by failing to employ reasonable measures to secure employees' PII.

134. This Court also should issue corresponding prospective injunctive relief requiring Wabtec to employ adequate security protocols consistent with law and industry standards to protect employees' PII.

135. If an injunction is not issued, Plaintiffs will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Wabtec. The risk of another such breach is real, immediate, and substantial. If another breach at Wabtec occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

136. The hardship to Plaintiffs if an injunction is not issued exceeds the hardship to Wabtec if an injunction is issued. Plaintiffs will likely be subjected to substantial identity theft and

other damage. On the other hand, the cost to Wabtec of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Wabtec has a pre-existing legal obligation to employ such measures.

137. Issuance of the requested injunction will not disserve the public interest. In contrast, such an injunction would benefit the public by preventing another data breach at Wabtec, thus eliminating the additional injuries that would result to Plaintiffs and employees whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all other similarly situated, pray for relief as follows:

a. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiffs as representative of the Class and Plaintiffs' attorneys as Class Counsel to represent the Class;

b. For an order finding in favor of Plaintiffs and the Class on all counts asserted herein;

c. For damages in an amount to be determined by the trier of fact;

d. For an order of restitution and all other forms of equitable monetary relief;

e. Declaratory and injunctive relief as described herein;

f. Awarding Plaintiffs' reasonable attorneys' fees, costs, and expenses;

g. Awarding pre- and post-judgment interest on any amounts awarded; and

h. Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMANDED

A jury trial is demanded on all claims so triable.

Dated: June 26, 2023

Respectfully submitted,

/s/ Gary F. Lynch
Gary F. Lynch
Kelly K. Iverson
Nicholas A. Colella
LYNCH CARPENTER LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
P: (412) 322-9243
gary@lcllp.com
kelly@lcllp.com
nickc@lcllp.com

/s/ Marc E. Dann
Marc E. Dann (*pro hac vice* forthcoming)
Brian D. Flick (*pro hac vice* forthcoming)
DANNLAW
15000 Madison Ave.
Lakewood, OH 44107
P: (216) 373-0539
notices@dannlaw.com

Counsel for Plaintiffs